Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in

the application:

<u>Listing of Claims:</u>

1. (currently amended) A circuit for generating a cipher stream, the

circuit comprising:

a first and a second plurality of linear feedback shift registers (LFSR),

a first of the second plurality of LFSR having a clock signal as a clock input

and others of the first second plurality of LFSR each having an output of another a

previous one of the first second plurality of LFSR as a clock input;

a first of the first plurality of LFSR having the clock signal combined with an

output of the first of the second plurality of LFSR as a clock input and others of the

second first plurality of LFSR each having an output of a previous one of the first

second plurality of LSFR combined with an output of another a previous one of the

first plurality of LFSR as a clock input; and

an output of a last of the first plurality of LFSR and an output of a last of the

second plurality of LFSR being combined to produce the cipher stream.

- 2 -

**Applicant:** Fatih M. Ozluturk **Application No.:** 10/803,263

2. (original) The circuit of claim 1 wherein the first plurality of LFSR

numbers a same value as the second plurality of LFSR.

3. (currently amended) The circuit of claim 1 wherein the combining of

the output of a previous one of the first second plurality of LSFR with an output of

another of another a previous one of the first plurality of LSFR is performed by an

AND gate.

4. (currently amended) The circuit of claim 1 wherein the output of the

last of the first plurality of LFSR and the output of the last of the second plurality of

LFSR is <u>combined</u> by an exclusive-or gate.

5. (currently amended) Software configured to produce a cipher stream,

the software effectively modeling a circuit having components comprising:

a first and a second plurality of linear feedback shift registers (LFSR),

a first of the second plurality of LFSR having a clock signal as a clock input

and others of the first second plurality of LFSR each having an output of another a

previous one of the first second plurality of LFSR as a clock input;

a first of the first plurality of LFSR having the clock signal combined with an

output of the first of the second plurality of LFSR as a clock input and others of the

. 3 -

**Applicant:** Fatih M. Ozluturk

**Application No.:** 10/803,263

second first plurality of LFSR each having an output of one a previous one of the

first second plurality of LSFR combined with an output of another a previous one of

the first plurality of LFSR as a clock input; and

an output of a last of the first plurality of LFSR and an output of a last of the

second plurality of LFSR being combined to produce the cipher stream.

(original) The software of claim 5 wherein the first plurality of LFSR 6.

numbers a same value as the second plurality of LFSR.

7. (currently amended) The software of claim 5 wherein the combining of

the output of one of the first plurality of LSFR with an output of another of another

of the first plurality of LSFR is performed by an AND gate.

8. (currently amended) The software of claim 5 wherein the output of the

last of the first plurality of LFSR and the output of the last of the second plurality of

LFSR is <u>combined</u> by an exclusive-or gate.

- 4 -